Home (https://www.bleepingcomputer.com/)
> News (https://www.bleepingcomputer.com/news/)
> Security (https://www.bleepingcomputer.com/news/security/)
> AnyDesk says hackers breached its production servers, reset passwords

AnyDesk says hackers breached its production servers, reset passwords

By
Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)
February 2, 2024 05:16 PM **13**

AnyDesk confirmed today that it suffered a recent cyberattack that allowed hackers to gain access to the company's production systems. BleepingComputer has learned that source code and private code signing keys were stolen during the attack.

AnyDesk is a remote access solution that allows users to remotely access computers over a network or the internet. The program is very popular with the enterprise, which use it for remote support or to access colocated servers.

The software is also popular among threat actors who use it for persistent access to breached devices and networks (https://www.bleepingcomputer.com/news/security/rackspace-confirms-play-ransomware-was-behind-recent-cyberattack/).

The company reports having 170,000 customers, including 7-Eleven, Comcast, Samsung, MIT, NVIDIA, SIEMENS, and the United Nations.

AnyDesk hacked

In a statement shared with BleepingComputer late Friday afternoon, AnyDesk says they first learned of the attack after detecting indications of an incident on their production servers.

After conducting a security audit, they determined their systems were compromised and activated a response plan with the help of cybersecurity firm CrowdStrike.

AnyDesk did not share details on whether data was stolen during the attack. However, BleepingComputer has learned that the threat actors stole source code and code signing certificates.

The company also confirmed ransomware was not involved but didn't share too much information about the attack other than saying their servers were breached, with the advisory mainly focusing on how they responded to the incident.

As part of their response, AnyDesk says they have revoked security-related certificates and remediated or replaced systems as necessary. They also reassured customers that AnyDesk was safe to use and that there was no evidence of end-user devices being affected by the incident.

"We can confirm that the situation is under control and it is safe to use AnyDesk. Please ensure that you are using the latest version, with the new code signing certificate," AnyDesk said in a public statement (https://anydesk.com/en/public-statement).

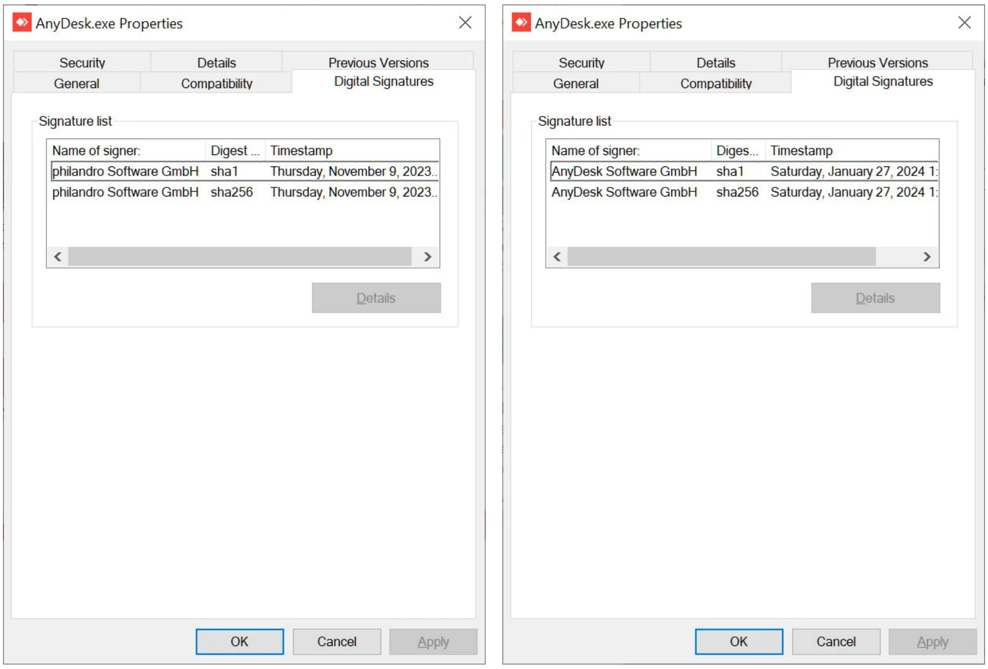
While the company says that no authentication tokens were stolen, out of caution, AnyDesk is revoking all passwords to their web portal and suggests changing the password if it's used on other sites.

"AnyDesk is designed in a way which session authentication tokens cannot be stolen. They only exist on the end user's device and are associated with the device fingerprint. These tokens never touch our systems, "AnyDesk told BleepingComputer in response to our questions about the attack.

"We have no indication of session hijacking as to our knowledge this is not possible."

The company has already begun replacing stolen code signing certificates, with Günter Born of BornCity first reporting (http://www.borncity.com/blog/2024/02/01/anydesk-und-diestoerungen-es-ist-womoeglich-was-im-busch/) that they are using a new certificate in AnyDesk version 8.0.8, released on January 29th. The only listed change in the new version is that the company switched to a new code signing certificate and will revoke the old one soon.

BleepingComputer looked at previous versions of the software, and the older executables were signed under the name 'philandro Software GmbH' with serial number 0dbf152deaf0b981a8a938d53f769db8. The new version is now signed under 'AnyDesk Software GmbH,' with a serial number of 0a8177fcd8936a91b5e0eddf995b0ba5, as shown below.



Name of signer:	Digest ...	Timestamp
philandro Software GmbH	sha1	Thursday, November 9, 2023...
philandro Software GmbH	sha256	Thursday, November 9, 2023...

Name of signer:	Diges...	Timestamp
AnyDesk Software GmbH	sha1	Saturday, January 27, 2024 1:
AnyDesk Software GmbH	sha256	Saturday, January 27, 2024 1:

Signed AnyDesk 8.0.6 (left) vs AnyDesk 8.0.8 (right)

Source: BleepingComputer

Certificates are usually not invalidated unless they have been compromised, such as being stolen in attacks or publicly exposed.

While AnyDesk had not shared when the breach occurred, Born reported that AnyDesk suffered a four-day outage starting on January 29th, during which the company disabled the ability to log in to the AnyDesk client.

"my.anydesk II is currently undergoing maintenance, which is expected to last for the next 48 hours or less," reads the AnyDesk status message page (https://status.anydesk.com/).

"You can still access and use your account normally. Logging in to the AnyDesk client will be restored once the maintenance is complete."

Yesterday, access was restored, allowing users to log in to their accounts, but AnyDesk did not provide any reason for the maintenance in the status updates.

However, AnyDesk has confirmed to BleepingComputer that this maintenance is related to the cybersecurity incident.

It is strongly recommended that all users switch to the new version of the software, as the old code signing certificate will soon be revoked.

Furthermore, while AnyDesk says that passwords were not stolen in the attack, the threat actors did gain access to production systems, so it is strongly advised that all AnyDesk users change their passwords. Furthermore, if they use their AnyDesk password at other sites, they should be changed there as well.

Every week, it feels like we learn of a new breach against well-known companies.

Last night, Cloudflare disclosed that they were hacked (https://www.bleepingcomputer.com/news/security/cloudflare-hacked-using-auth-tokens-stolen-in-okta-attack/) on Thanksgiving using authentication keys stolen during last years Okta cyberattack (https://www.bleepingcomputer.com/news/security/okta-says-its-support-system-was-breached-using-stolen-credentials/).

Last week, Microsoft also revealed that they were hacked by Russian state-sponsored hackers (https://www.bleepingcomputer.com/news/security/microsoft-reveals-how-hackers-breached-its-exchange-online-accounts/) named Midnight Blizzard, who also attacked HPE (https://www.bleepingcomputer.com/news/security/hpe-russian-hackers-breached-its-security-teams-email-accounts/) in May.

Related Articles:

GTA 5 source code reportedly leaked online a year after Rockstar hack (https://www.bleepingcomputer.com/news/security/gta-5-source-code-reportedly-leaked-online-a-year-after-rockstar-hack/)

German battery maker Varta halts production after cyberattack (https://www.bleepingcomputer.com/news/security/german-battery-maker-varta-halts-production-after-cyberattack/)

Prudential Financial breached in data theft cyberattack (https://www.bleepingcomputer.com/news/security/prudential-financial-breached-in-data-theft-cyberattack/)

Lurie Children's Hospital took systems offline after cyberattack (https://www.bleepingcomputer.com/news/security/lurie-childrens-hospital-took-systems-offline-after-cyberattack/)

Johnson Controls says ransomware attack cost $27 million, data stolen (https://www.bleepingcomputer.com/news/security/johnson-controls-says-ransomware-attack-cost-27-million-data-stolen/)

ANYDESK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ANYDESK/)

CODE SIGNING CERTIFICATE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CODE-SIGNING-CERTIFICATE/)

CYBERATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBERATTACK/)

SOURCE CODE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SOURCE-CODE/)